

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-22680

(P2000-22680A)

(43)公開日 平成12年1月21日(2000.1.21)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード* (参考)
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 B
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 Z
	17/60	G 0 9 C 1/00	6 2 0 Z
G 0 9 C 1/00	6 2 0		6 4 0 C
	6 4 0	G 0 6 F 15/21	3 3 0

審査請求 未請求 請求項の数7 O L (全 11 頁)

(21)出願番号 特願平10-191706

(22)出願日 平成10年7月7日(1998.7.7)

(71)出願人 598090519

株式会社オープンループ

北海道札幌市清田区清田七条一丁目18番5号

(72)発明者 浅田 一憲

北海道札幌市清田区北野7条2丁目5番5号 株式会社オープンループ内

(74)代理人 100095407

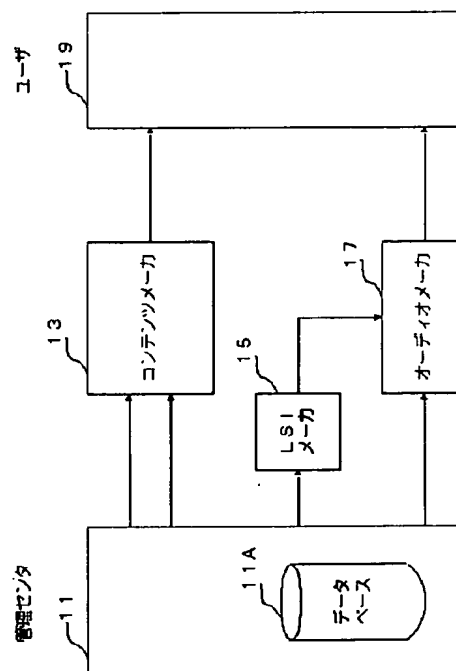
弁理士 木村 満 (外2名)

(54)【発明の名称】 デジタルコンテンツ流通方法及びコンテンツを再生可能に記録した記録媒体

(57)【要約】

【課題】 音楽等のデジタルコンテンツの不正コピー利用を防止し、安全に流通させる。

【解決手段】 管理センタ11は、マスタ公開鍵KPUkをコンテンツメーカー13に供給し、マスタープライベート鍵KPRkをLSIメーカ15に供給する。コンテンツメーカー13は、コンテンツ別にコンテンツ暗号鍵Kcoを生成して暗号化したデータと、コンテンツ暗号鍵Kcoをマスタ公開鍵KPUkにより暗号化したデータと、自己の署名と、管理センタ11からの証明書DVとを記録媒体21に記録する。LSIメーカ15は、暗号化されたコンテンツ暗号鍵を復号するためのマスタープライベート鍵KPRkを復号LSIに含める。復号機器は、復号LSIにより、装着された記録媒体21の証明書DVと署名DSが共に有効であると判断した際に、マスタープライベート鍵KPRkによりコンテンツ暗号鍵を復号し、コンテンツを復号する。



#### 【特許請求の範囲】

【請求項1】 デジタルコンテンツの流通を管理する管理センタと、前記管理センタの管理下に、デジタルコンテンツを暗号化して流通させるコンテンツメーカーと、前記コンテンツメーカーが提供するコンテンツを復号して利用可能とする復号手段を提供する復号手段提供手段と、を備える流通システムを用いてデジタルコンテンツを流通する方法であって、

前記コンテンツメーカーは、コンテンツ別に生成されたコンテンツ暗号鍵によりコンテンツを暗号化し、前記管理センタは、暗号化されたコンテンツ暗号鍵を記録媒体に記録するための情報をコンテンツメーカーに提供し、

前記コンテンツメーカーは、コンテンツ暗号鍵により暗号化されたコンテンツと、暗号化されたコンテンツ暗号鍵とを記録媒体に記録して流通させ、

前記管理センタは、暗号化されたコンテンツ暗号鍵を復号するための復号情報を復号手段提供手段に提供し、前記復号手段提供手段は、前記暗号化されたコンテンツ暗号鍵を復号するための復号情報を前記復号手段に含め、

前記復号手段は、前記記録媒体に記録されているコンテンツ暗号鍵を前記復号情報を用いて復号し、復号した暗号鍵で、コンテンツを復号して再生する、ことを特徴とするデジタルコンテンツ流通方法。

【請求項2】 前記コンテンツメーカーは、コンテンツ別にコンテンツ暗号鍵を生成してコンテンツを暗号化し、生成したコンテンツ暗号鍵を管理センタから供給されたマスタ公開鍵により暗号化し、管理センタから供給された署名用コンテンツメーカープライベート鍵を用いて自己の署名を作成し、暗号化したコンテンツと暗号化したコンテンツ暗号鍵と署名と管理センタから供給された証明書とを記録媒体に格納し、

前記復号手段提供手段は、前記復号手段に、暗号化されたコンテンツ暗号鍵を復号するためのマスタプライベート鍵と、証明書を検証するための署名用センタ公開鍵とを含め、

前記復号手段は、証明書を署名用センタ公開鍵を用いて検証することにより、コンテンツメーカーの署名用コンテンツメーカー公開鍵を得て、これにより署名を検証し、証明書及び署名が共に有効であると判断した際に、前記マスタプライベート鍵により暗号化コンテンツ暗号鍵を復号し、復号したコンテンツ暗号化鍵により、コンテンツを復号し、

前記管理センタは、マスタ公開鍵と、コンテンツメーカーの署名用コンテンツメーカー公開鍵を署名用センタプライベート鍵で暗号化した情報を含む証明書とをコンテンツメーカーに供給し、マスタプライベート鍵と署名用センタ公開鍵を前記復号手段提供手段に供給する、ことを特徴とする請求項1に記載のデジタルコンテン

ツ流通方法。

【請求項3】 前記コンテンツメーカーは、コンテンツ別にコンテンツ暗号鍵を生成してコンテンツを暗号化し、生成したコンテンツ暗号鍵を管理センタに供給し、管理センタから供給された署名用コンテンツメーカープライベート鍵を用いて自己の署名を作成し、暗号化されたコンテンツと、管理センタより供給されたマスタ暗号鍵により暗号化されているコンテンツ暗号鍵と、署名と、管理センタから提供された証明書とを記録媒体に記録し、前記復号手段提供手段は、前記復号手段に、マスタ暗号鍵と、証明書を検証するための署名用センタ公開鍵とを含め、

前記復号手段は、証明書を署名用センタ公開鍵を用いて検証することにより、コンテンツメーカーの署名用コンテンツメーカー公開鍵を得て、これにより署名を検証し、証明書及び署名が共に有効であると判断した際に、前記マスタ暗号鍵により暗号化コンテンツ暗号鍵を復号し、復号したコンテンツ暗号化鍵により、コンテンツを復号し、

前記管理センタは、コンテンツメーカーの署名用コンテンツメーカー公開鍵を署名用センタプライベート鍵で暗号化した情報を含む証明書と、コンテンツメーカーから供給されたコンテンツ暗号鍵をマスタ暗号鍵で暗号化したデータとをコンテンツメーカーに供給し、マスタ暗号鍵と署名用センタ公開鍵を前記復号手段提供手段に供給する、ことを特徴とする請求項1に記載のデジタルコンテンツ流通方法。

【請求項4】 前記復号手段は、前記暗号化されたコンテンツ暗号鍵を復号するための情報を記憶し、この情報によりコンテンツ暗号鍵を復号し、復号したコンテンツ暗号鍵を用いて暗号化されたコンテンツを復号するLSI（大規模集積回路）と、前記暗号化されたコンテンツ暗号鍵を復号するための情報を含み、この情報によりコンテンツ暗号鍵を復号し、復号したコンテンツ暗号鍵を用いて暗号化されたコンテンツを復号するソフトウェアと、の少なくとも一方を備える、

ことを特徴とする請求項1、2又は3に記載のデジタルコンテンツ流通方法。

【請求項5】 前記コンテンツメーカーは、各コンテンツの一部を平文で記録し、他の少なくとも一部を前記コンテンツ暗号鍵により暗号化して前記記録媒体に記録する、ことを特徴とする請求項1、2、3又は4に記載のデジタルコンテンツ流通方法。

【請求項6】 複数のデジタルコンテンツが記録された記録媒体であって、

コンテンツ毎に、その少なくとも一部が、コンテンツ別の第1の暗号化鍵で暗号化されたデジタルコンテンツと、第2の暗号化鍵により暗号化された前記第1の暗号化鍵

と、製造者のプライベート鍵を用いて生成されたデジタル署名と、前記製造者のデジタル署名を検証するための製造者の公開鍵を含む所定機関の証明書と、が記録されていることを特徴とするデジタルコンテンツ記録媒体。

【請求項7】各デジタルコンテンツは、その一部が平文で、少なくとも他の一部が第1の暗号化鍵で暗号化されて記録媒体に記録されている、ことを特徴とする請求項6に記載のデジタルコンテンツ記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、著作権等で保護されるコンテンツの保護と利用の調和を取ることを可能とするデジタルコンテンツ流通方式及びデジタルコンテンツを記録した記録媒体に関する。

【0002】

【従来の技術】デジタル画像処理技術の進歩により、種々のコンテンツを加工・編集・複製することが可能になりつつある。しかし、コンテンツの加工・編集・複製を無秩序に認めると、著作権や肖像権が保護されなくなり、権利者の利益が損なわれてしまう。一方、これらのコンテンツの利用を制限しすぎるとコンテンツが利用されなくなる。

【0003】これらの要件を満たすため、デジタルすかし等の技術も提案されているが、データ処理が複雑であり、複雑なシステムが要求される。このため、データ処理技術に習熟していない利用者の立場から簡便に利用できるシステムとはなっていない。

【0004】

【発明が解決しようとする課題】この発明は上記実状に鑑みてなされたもので、デジタルコンテンツの利用と保護の調和を図ることを目的とする。

【0005】

【課題を解決するための手段】上記目的を達成するため、この発明の第1の観点にかかるデジタルコンテンツ流通方法は、デジタルコンテンツの流通を管理する管理センタ(11)と、前記管理センタ(11)の管理下に、デジタルコンテンツを暗号化して流通させるコンテンツメーカ(13)と、前記コンテンツメーカ(13)が提供するコンテンツを復号して利用可能とする復号手段を提供する復号手段提供手段(15、17)と、を備える流通システムを用いてデジタルコンテンツを流通する方法であって、前記コンテンツメーカ(13)は、コンテンツ別に生成されたコンテンツ暗号鍵(Kco)によりコンテンツを暗号化し、前記管理センタ(11)は、暗号化されたコンテンツ暗号鍵(KPUk(Kco); Kk(Kco))を記録媒体(21)に記録するための情報(KPUk; Kk)をコンテンツメーカ(13)に提供し、前記コンテンツメーカ(13)は、コンテ

ツ暗号鍵(Kco)により暗号化されたコンテンツ(DC)と、暗号化されたコンテンツ暗号鍵(KPUk(Kco); Kk(Kco))とを記録媒体(21)に記録して流通させ、前記管理センタ(11)は、暗号化されたコンテンツ暗号鍵(KPUk(Kco); Kk(Kco))を復号するための復号情報(KPRk; Kk)を復号手段提供手段(15)に提供し、前記復号手段提供手段(15)は、前記暗号化されたコンテンツ暗号鍵を復号するための復号情報(KPRk; Kk)を前記復号手段(LS I etc)に含め、前記復号手段(LS I etc)は、前記記録媒体(21)に記録されているコンテンツ暗号鍵(Kco)を前記復号情報(KPRk; Kk)を用いて復号し、復号した暗号鍵(Kco)で、コンテンツを復号して再生する、ことを特徴とする。

【0006】この方法によれば、デジタルコンテンツを暗号化した状態で流通させて不正使用を防止し、さらに、再生することができる。鍵が、管理センタを中心として三者で管理されているので信頼性及び安全性が高い。さらに、コンテンツ別に暗号化鍵が異なるので、ある暗号化鍵が破られても、それが記録媒体全体に及ぶことがなく、安全である。

【0007】暗号化の方式として公開鍵方式を使用する場合は、次の構成が有効である。まず、前記コンテンツメーカは、コンテンツ別にコンテンツ暗号鍵を生成してコンテンツを暗号化し、生成したコンテンツ暗号鍵を管理センタから供給されたマスタ公開鍵(KPUk)により暗号化し、管理センタ(11)から供給された署名用コンテンツメーカプライベート鍵(KPRm)を用いて自己の署名を作成し、暗号化したコンテンツと暗号化したコンテンツ暗号鍵(KPUk(Kco))と署名(DS)と管理センタ(11)から供給された証明書(DV)とを記録媒体(21)に格納し、前記復号手段提供手段(15)は、前記復号手段(LS I)に、暗号化されたコンテンツ暗号鍵(KPUk(Kco))を復号するためのマスタプライベート鍵(KPRk)と、証明書(DV)を検証するための署名用センタ公開鍵(KPUce)とを含め、前記復号手段(LS I)は、証明書(DV)を署名用センタ公開鍵(KPUce)を用いて検証することにより、コンテンツメーカ(13)の署名用コンテンツメーカ公開鍵(KPUm)を得て、これにより署名(DS)を検証し、証明書(DV)及び署名(DS)が共に有効であると判断した際に、前記マスタプライベート鍵(KPRk)により暗号化コンテンツ暗号鍵(KPUk(Kco))を復号し、復号したコンテンツ暗号化鍵(Kco)により、コンテンツを復号し、前記管理センタ(11)は、マスタ公開鍵(KPUk)と、コンテンツメーカの署名用コンテンツメーカ公開鍵(KPUm)を署名用センタプライベート鍵(KPRce)で暗号化した情報(KPRce(KPUm))を含む証明書(DV)とをコンテンツメーカに供給し、マスタプライベート鍵(KPRk)と署名用センタ公開鍵

(KPUce)を前記復号手段提供手段(15)に供給する。この方法によれば、コンテンツ暗号鍵を暗号化するための鍵と復号するための鍵が別個に管理されているので、より安全である。さらに、署名及び証明書を用いることにより、その信頼性が高い。

【0008】暗号化の方式として秘密鍵方式を使用する場合は、次の構成が有効である。前記コンテンツメーカ(13)は、コンテンツ別にコンテンツ暗号鍵(Kco)を生成してコンテンツを暗号化し、生成したコンテンツ暗号鍵(Kco)を管理センタ(11)に供給し、管理センタ(11)から供給された署名用コンテンツメーカプライベート鍵(KPRm)を用いて自己の署名(DV)を作成し、暗号化されたコンテンツ(DC)と、管理センタ(11)より供給されたマスタ暗号鍵(Kk)により暗号化されているコンテンツ暗号鍵(Kk(Kco))と、署名(DV)と、管理センタから提供された証明書(DV)とを記録媒体(21)に記録し、前記復号手段提供手段(15)は、前記復号手段(LSI)に、マスタ暗号鍵(Kk)と、証明書(DV)を検証するための署名用センタ公開鍵(KPRce)とを含め、前記復号手段(LSI)は、証明書(DV)を署名用センタ公開鍵(KPRce)を用いて検証することにより、コンテンツメーカの署名用コンテンツメーカ公開鍵(KPUm)を得て、これにより署名(DS)を検証し、証明書(DV)及び署名(DS)が共に有効であると判断した際に、前記マスタ暗号鍵(Kk)により暗号化コンテンツ暗号鍵(Kk(Kco))を復号し、復号したコンテンツ暗号化鍵(Kco)により、コンテンツを復号し、前記管理センタ(11)は、コンテンツメーカ(13)の署名用コンテンツメーカ公開鍵(KPUm)を署名用センタプライベート鍵(KPRce)で暗号化した情報(KPRce(KPUm))を含む証明書(DV)と、コンテンツメーカ(13)から供給されたコンテンツ暗号鍵(Kco)をマスタ暗号鍵(Kk)で暗号化したデータとをコンテンツメーカ(13)に供給し、マスタ暗号鍵(Kk)と署名用センタ公開鍵(KPUce)を前記復号手段提供手段(15)に供給する。

【0009】この方法によれば、コンテンツ暗号鍵を暗号化するための鍵と復号するための鍵が共通であるので、復号時(再生時)の処理が高速に行うことができ、リアルタイム性が要求される用途に特に有効である。また、コンテンツ暗号化鍵を暗号化する処理がセンタで行われているため、秘密鍵方式を用いていながらその信頼性が非常に高い。さらに、署名及び証明書を用いることにより、その信頼性が高い。

【0010】前記復号手段は、前記暗号化されたコンテンツ暗号鍵(Kco)を復号するための情報(KPRk、Kk)を記憶し、この情報によりコンテンツ暗号鍵(Kco)を復号し、復号したコンテンツ暗号鍵(Kco)を用いて暗号化されたコンテンツを復号するLSIであっても、前記暗号化されたコンテンツ暗号鍵を復号するため

の情報を含み、この情報によりコンテンツ暗号鍵(Kco)を復号し、復号したコンテンツ暗号鍵(Kco)を用いて暗号化されたコンテンツを復号するソフトウェアであっても、よい。

【0011】前記コンテンツメーカは、各コンテンツの一部を平文で記録し、他の少なくとも一部を前記コンテンツ暗号鍵(Kco)により暗号化して前記記録媒体に記録するようにしてもよい。このようにすれば、曲の一部、例えば、イントロを聞いて曲を確認したり、営業用を使用するさせる等の行為が容易にできる。

【0012】上記目的を達成するため、この発明の第2の観点にかかる、複数のデジタルコンテンツが記録された記録媒体は、コンテンツ毎に、その少なくとも一部が、コンテンツ別の第1の暗号化鍵(Kco)で暗号化されたデジタルコンテンツと、第2の暗号化鍵(KPUk; Kk)により暗号化された前記第1の暗号化鍵(Kco)と、製造者のプライベート鍵を用いて生成されたデジタル署名(DS)と、前記製造者のデジタル署名を検証するための製造者の公開鍵(KPUm)を含む所定機関の証明書(DV)と、が記録されている、ことを特徴とする。

【0013】この構成によれば、証明書を確認する情報と第1の鍵を復号する情報を有する者以外の者は、即ち、正当権限を有していない者は、所定機関の証明を確認し、さらに、その確認結果から製造者の署名を確認し、そして、コンテンツを復号することができない。従って、デジタルデータを安全に市場に流通させることができる。

【0014】各デジタルコンテンツは、その一部が平文で、少なくとも他の一部が第1の暗号化鍵で暗号化されて記録媒体に記録されてもよい。

【0015】

【発明の実施の形態】この発明の実施の形態にかかるコンテンツ流通システム及び方法を、オーディオデータ(音楽データ)を流通させる場合を例に説明する。

(第1の実施の形態)この実施の形態のコンテンツ流通システムは、図1に示すように、管理センタ11と、コンテンツメーカ13と、LSI(大規模集積回路)メーカ15と、オーディオメーカ(音響機器メーカ)17と、ユーザ19とを含む。

【0016】管理センタ11は、暗号化技術を有し、暗号化対象コンテンツの特質及び顧客の要求に応じて暗号ファイルフォーマットを設定すると共に各種暗号鍵を生成し、コンテンツメーカ13とLSIメーカ15に供給する。管理センタ11は、データベース11Aにより、顧客又は契約別に暗号ファイルフォーマット及び暗号鍵を記録して、管理する。管理センタ11が発生する暗号鍵については図2を参照してまとめて説明する。

【0017】コンテンツメーカ13は、管理センタ11の暗号ファイルフォーマットの使用許諾に基づき、コン

テンツ毎に暗号化鍵を生成してコンテンツ（ここでは、音楽データ）を暗号化し、記録媒体（例えば、フラッシュメモリ）などに格納して販売する。

【0018】LSIメカ15は、管理センタ11の暗号ファイルフォーマットの使用許諾に基づき、ASIC（特定用途向け集積回路）技術により、管理センタ11が設定した暗号ファイルフォーマット及び提供された暗号鍵に従って暗号化されたコンテンツを復号する復号LSIを設計・製造し、販売する。

【0019】復号LSIは、オーディオメカ17に販売される。オーディオメカ17は、管理センタ11の暗号ファイルフォーマットの使用許諾に基づき、復号LSIを組み込み、コンテンツメカ13が提供する媒体に記録されているコンテンツデータを復号し、再生する装置（オーディオ機器）を製造し、販売する。

【0020】管理センタ11は、例えば、コンテンツメカ13、LSIメカ15、オーディオメカ17からの対価を運営資金の全部又は一部として運営される。

【0021】ユーザ19は、オーディオメカ17が提供するオーディオ機器と、コンテンツメカ13が提供する音楽データを格納した記録媒体とを購入し、オーディオ機器に記録媒体を装着して、音楽データを再生する。記録媒体から再生された音楽データは暗号化されたデータであるが、復号LSIにより復号され、音楽として再生される。

【0022】次に、この流通システムで使用される各暗号鍵について図2を参照して説明する。コンテンツ鍵Kcoは、コンテンツメカ13がコンテンツ毎に乱数を発生させて生成する暗号鍵であり、流通対象のコンテンツを暗号化するためにコンテンツメカが使用する。

【0023】マスタ公開鍵KPUkは、管理センタ11が、例えば、コンテンツメカ毎（コンテンツ毎等でも可）に発生して供給する暗号鍵であり、供給を受けたコンテンツメカ13がコンテンツ鍵Kcoを暗号化するために使用する。

【0024】マスタプライベート鍵KPRkは、管理センタ11が、マスタ公開鍵KPUkと対で発生し、各LSIメカ15に供給する暗号化鍵であり、復号用LSIや復号用ソフトウェアに格納され、マスタ公開鍵KPUkにより暗号化されたコンテンツ鍵Kcoを復号するために使用される。

【0025】署名用コンテンツメカプライベート鍵KPRmは、管理センタ11がコンテンツメカ毎に発生して提供する暗号鍵であり、コンテンツメカが各コンテンツに署名するために使用される。

【0026】署名用コンテンツメカ公開鍵KPUmは、管理センタ11が署名用コンテンツメカプライベート鍵KPRmと対で発生し、コンテンツメカの署名を検証するために、管理センタ11が発行する証明書に含めて使用される。

【0027】署名用センタプライベート鍵KPRceは、管理センタ11が自ら発生し、各コンテンツメカの署名用コンテンツメカ公開鍵KPUmを暗号化して「コンテンツメカ鍵証明書」を生成するために使用される。

【0028】署名用センタ公開鍵KPUceは、管理センタ11が、署名用センタプライベート鍵KPRceと対で発生する鍵であり、復号LSIに格納され、「コンテンツメカ鍵証明書」内にある管理センタ11の署名を検証するために使用される。

【0029】次に、コンテンツメカ13が提供する音楽データについて説明する。図3に、記録媒体21に格納される音楽データの構成例を示す。各媒体の先頭位置には、その媒体の識別コード、コンテンツメカ13の識別コード、媒体のタイプ、TOC（TABLE OF CONTENTS）情報、著作権情報等の制御情報DZと、N曲分の音楽のデータが記録されている。

【0030】各曲のデータは、識別コードDIと、平文データDPと、暗号化データDCと、暗号化コンテンツ鍵DKと、コンテンツメカの署名DSと、証明書DVから構成されている。

【0031】識別コードDIは、各曲の曲名、曲コード、演奏時間等を示す暗号化されていない平文データである。

【0032】平文データDPは、楽曲データのうちの前半の所定時間（例えば、10秒程度）分の暗号化されない平文データである。

【0033】暗号化データDCは、楽曲データの後半の部分が、このコンテンツ用のコンテンツ鍵Kcoで暗号化されて生成されたデータである。

【0034】暗号化コンテンツ鍵DKは、コンテンツ鍵Kcoをマスタ公開鍵KPUkで暗号化して得られたデータKPUk（Kco）である。

【0035】コンテンツメカの署名DSは、識別コードDIと、平文データDPと、暗号化データDCと、暗号化コンテンツ鍵DKと、をハッシュ関数等の一方方向性関数H（）で変換し、これをコンテンツメカプライベート鍵KPRmで暗号化して得られたデータKPRm（H（DI；DP；DC；DK））である。

【0036】鍵証明書DVは、署名用コンテンツメカ公開鍵KPUmと、この署名用コンテンツメカ公開鍵KPUmを署名用センタプライベート鍵KPRceで暗号化して得られたデータKPRce（KPUm）とを含み、コンテンツメカが署名に使用した鍵が正当なものであることを管理センタ11が証明するためのものである。

【0037】次に、復号LSIについて説明する。復号LSI31は、図4に示すように、ドライバ33、署名確認部34、CPUリセット部35、復号部36、記憶部37、制御部38を備える。

【0038】ドライバ33は、記録媒体21の記録データを順次読み出す。署名確認部34は、復号対象のコン

テンツに証明書DV及び署名DSが付されているか否かを判別し、付されていると判別すると、証明書DVと署名DSを検証する。

【0039】即ち、署名確認部34は、ドライバ33が読み出した証明書DVのうち、暗号化されている部分KPRce (KPUm) を、記憶部37に記憶されている管理センタ11の署名用センタ公開鍵KPUceを用いて復号して、署名用コンテンツメーカー公開鍵KPUmを得る。署名確認部34は、復号した署名用コンテンツメーカー公開鍵KPUmと平文の署名用コンテンツメーカー公開鍵KPUmとを比較し、一致するか否かを判別する。

【0040】一致すると判別すると、この署名用コンテンツメーカー公開鍵KPUmを用いてコンテンツメーカーの署名DSを検証する。即ち、署名用コンテンツメーカー公開鍵KPUmを用いて復号した署名DSと、識別コードDIと、平文データDPと、暗号化データDCと、暗号化コンテンツ鍵DKとを所定の一方方向性関数H ( ) で変換したものが一致するか否かを判別する。署名確認部34は、一致すると判別すると、暗号化コンテンツ鍵DK (=KPUk (Kco) ) をマスタプライベート鍵KPRkを用いて復号し、コンテンツ鍵Kcoを再生する。

【0041】CPUリセット部35は、署名確認部34が署名又は証明書を検出できなかった（署名又は証明書が存在しなかった）場合及び検証を認証できなかった（存在したが、認証できなかった）場合には、データの再生を禁止するため、復号LSI31が組み込まれている装置（再生装置）のCPU45をリセットする。これにより、再生動作は、キャンセルされる。

【0042】復号部36は、署名確認部34が署名を認証した場合に、ドライバ33が読み出すデータを復号する部分であり、平文データについてはそのまま再生し、暗号化されているデータについては、署名確認部34が復号したコンテンツ鍵Kcoを用いて音楽データDDを復号する。記憶部37は、管理センタ11の署名用センタ公開鍵KPUceと、コンテンツメーカー13毎のマスタプライベート鍵KPRkとを記憶する。

【0043】このシステムを有効に運用するためには、記憶部37が記憶している鍵KPUceとKPRkとは厳重に秘密状態に保持する必要がある。このため、記憶部37は、復号LSI31の外部から直接アクセスされないように、他の共通バスとは異なる内部バスにより署名確認部と接続されている。また、これらの鍵のデータが外部にそのまま出力されることはない。

【0044】制御部38は、この復号LSI31内の各部の動作を制御する。

【0045】次に、この復号LSI31を用いたオーディオ装置の構成について説明する。図4に示すように、このオーディオ装置は、記録媒体が着脱可能に装着されるコネクタ41と、コネクタ41を介して記録媒体21に接続された前述の復号LSI31と、復号LSI31

から出力される音楽データをアナログデータに変換するD/A変換器42と、D/A変換器42の出力するアナログ信号を放音するスピーカ（ヘッドフォン等を含む）43と、入力部44と、このオーディオ装置全体の動作を制御するCPU（制御部）45とから構成される。

【0046】コネクタ41には、記録媒体21が着脱可能に装着される。D/A変換器42は、再生されたデジタルオーディオ信号をアナログオーディオ信号に変換して出力する。スピーカ43は、アナログオーディオ信号を放音する。CPU45は、入力部44からの入力に従って、記録媒体21からのデータの読み出し・再生を含むこのシステム全体の動作を制御する。

【0047】次に、この流通システムを用いたデジタルコンテンツの流通方法について説明する。音楽を記録した記録媒体21を製造したいコンテンツメーカー13及びその記録媒体を再生するオーディオ機器を製造したいオーディオメーカー17は管理センタ11に登録する。

【0048】管理センタ11は、コンテンツメーカー13に暗号化フォーマットの使用を許可する場合には、暗号化フォーマットの使用を許諾し、そのノウハウを提供すると共にマスタ公開鍵KPUkと署名用プライベート鍵KPRmの対を提供する。また、証明用コンテンツメーカー公開鍵KPUmと、証明用コンテンツメーカー公開鍵KPUmを署名用センタプライベート鍵KPRceを用いて暗号化したデータKPRce (KPUm) とからなる証明書 (KPUm : KPRce (KPUm) ) を作成し、コンテンツメーカー13に送付する。コンテンツメーカー13は、管理センタ11に対し、一定のローヤリティ（対価）を支払う。

【0049】また、管理センタ11は、LSIメーカー15に暗号ファイルフォーマットに準拠した復号LSIの製造を許可する場合には、その許可とノウハウを提供すると共に各コンテンツメーカーのマスタプライベート鍵KPRkと自己の署名用センタ公開鍵KPUceを通知する。LSIメーカー15は、管理センタ11に対し、一定のローヤリティを支払う。

【0050】また、管理センタ11は、オーディオメーカー17に暗号化フォーマットの使用を許可する場合には、暗号化フォーマットの使用許可を与えると共にそのノウハウを提供する。オーディオメーカー17は、管理センタ11に対し、一定のローヤリティを支払う。

【0051】以下、コンテンツメーカーによる記録媒体21へのコンテンツの記録動作を図5のフローチャートを参照して説明する。まず、コンテンツメーカー13は、例えば、記録媒体に記憶させるコンテンツ毎、即ち、楽曲毎に乱数を発生してコンテンツ鍵Kcoを生成する（ステップS1）。次に、その曲の識別コード、制御コードの識別データDIを生成する（ステップS2）。

【0052】さらに、記録する楽曲の所定量の先頭部分DPを平文のまま残し、残りの部分DCをコンテンツ鍵Kcoで暗号化する（ステップS3）。ステップS1で生

成したコンテンツ鍵 $K_{co}$ を、マスタ公開鍵 $K_{PUk}$ で暗号化して暗号化コンテンツ鍵 $D_K$ を生成する（ステップS 4）。

【0053】さらに、上述のデータ全体、即ち、識別データ $D_I$ と、平文データ $D_P$ と、暗号化データ $D_C$ と、暗号化（暗号化された）コンテンツ鍵 $K_{PUk}$ （ $K_{co}$ ）とを、ハッシュ関数等の一方方向性関数 $H()$ を用いて変換し、さらに、変換結果を署名用コンテンツメーカプライベート鍵 $K_{PRm}$ で暗号化して、コンテンツメーカの署名 $D_S (=K_{PRm}(H(D_I; D_P; D_C; K_{PUk}(K_{co})))$ を生成する（ステップS 5）。

【0054】さらに、以上のデータに、管理センタ11から提供されている証明書 $D_V$ を付加して（ステップS 6）、1曲文のデータが完成する。コンテンツメーカ13は、このようにして生成した1曲分のデータを $N$ 曲分適宜組み合わせ（ステップS 7）、1記録媒体分のデータを生成し、これを記録媒体21に記録し（ステップS 8）、市場に流通させる（販売する）。なお、記録対象のデータを一旦メモリ上に作成すれば、そのデータを記録媒体に記録するだけで処理は完了する。

【0055】一方、許可を受けた $L S I$ メーカ13は、提供されたフォーマットに従って、ドライバ33等を備える復号 $L S I 31$ を $A S I C$ 技術等を用いて製造する。この際、記憶部37には、管理センタ11の署名用センタ公開鍵 $K_{PUc}$ と、コンテンツメーカ13の識別コードとマスタプライベート鍵 $K_{PRk}$ との対を記録させる。

【0056】許可を受けた音響オーディオメーカ15は、 $L S I$ メーカ15より復号 $L S I 31$ を購入し、図4に示すような音響装置を製造する。

【0057】オーディオメーカ17より音響機器を購入し、コンテンツメーカ13より記録媒体を購入したユーザ19は、図4に示すように記録媒体21を音響機器のコネクタ41に装着する。

【0058】以後、コンテンツの再生は図6のフローチャートに示すような手順で行われる。まず、入力部44から再生の指示及びその曲番が指定されると、 $C P U 45$ は復号 $L S I 31$ のドライバ33を制御してデータを読み出し、その曲の位置やコンテンツメーカの識別コードを制御情報 $D_Z$ から判別し（ステップS 11）、該当記憶位置からその曲のデータ全体を読み出す（ステップS 12）。

【0059】署名確認部34は、読み出したデータから、復号（再生）対象のコンテンツに管理センタ11の証明書 $D_V$ 及びコンテンツメーカ13の署名 $D_S$ が付されているか否かを判別し（ステップS 13）、少なくとも一方が付されていないと判別すると、コンテンツの再生を防止するため、 $C P U$ リセット部35を介して $C P U 45$ をリセットする（ステップS 14）。一方、ステップS 13で、証明書 $D_V$ 及び署名 $D_S$ が付されている

と判別すると、証明書 $D_V$ と署名 $D_S$ を検証する（ステップS 15～S 21）。

【0060】即ち、署名確認部34は、ドライバ33が読み出した証明書 $D_V$ のうち、署名用コンテンツメーカ公開鍵 $K_{PUm}$ が署名用センタプライベート鍵 $K_{PRce}$ で暗号化されている部分 $K_{PRce}(K_{PUm})$ を、記憶部37に格納されている署名用センタ公開鍵 $K_{PUce}$ で復号し（ステップS 15）、証明書 $D_V$ 内に平文で格納されている署名用コンテンツメーカ公開鍵 $K_{PUm}$ と一致するか否かを判別する（ステップS 16）。一致しないと判別したときは、証明書 $D_V$ は無効であり、 $C P U 45$ をリセットする（ステップS 14）。

【0061】一方、ステップS 16で、一致していると判別されると、証明書 $D_V$ は有効であり、証明書 $D_V$ に含まれていた署名用コンテンツメーカ公開鍵 $K_{PUm}$ を用いて、署名 $D_S$ を検証する。

【0062】まず、署名用コンテンツメーカ公開鍵 $K_{PUm}$ を用いて署名を復号する（ステップS 17）。次に、識別コード $D_I$ 、平文データ $D_P$ 、暗号化データ $D_C$ 、暗号化コンテンツ鍵 $D_K$ とを所定のハッシュ関数 $H()$ で変換する（ステップS 18）。

【0063】次に、ステップS 17で復号した内容とステップS 18でハッシュ関数 $H()$ で変換したデータが一致するか否かを判別する（ステップS 19）。一致しなければ、署名は無効であり、 $C P U 45$ をリセットする（ステップS 14）。

【0064】ステップS 19で一致すると判別された場合、即ち、証明書 $D_V$ も署名 $D_S$ も有効である（暗号化鍵が正しい）と判別された場合には、署名確認部34は、暗号化コンテンツ鍵 $D_K (=K_{PUk}(K_{co}))$ を記憶部37に格納されているそのコンテンツメーカ13のマスタプライベート鍵 $K_{PRk}$ を用いて復号し、コンテンツ鍵 $K_{co}$ を再生する（ステップS 20）。

【0065】署名確認部34は、復号部36に復号したコンテンツ鍵 $K_{co}$ を提供すると共に復号指示信号を送出する。

【0066】復号部36は、復号指示信号に応答し、ドライバ33が読み出した各曲の平文データをそのまま出力し、暗号化部分 $D_C$ をコンテンツ鍵 $K_{co}$ を用いて復号して、出力する。この出力データは $D/A$ 変換器47によりアナログ信号に変換され、スピーカ48から放音される。

【0067】このような構成によれば、デジタルコンテンツを暗号化して流通し、専用の $L S I$ を有する装置でのみ再生できるように構成したので、デジタルコンテンツの不正な複製を防止することができる。また、管理センタ11に登録するだけで、何人も実質的に共通の暗号ファイルフォーマットに準拠した製品を製造・販売することができる。さらに、コンテンツ単位で暗号化鍵が異なっているので、例え、一部の暗号化鍵が破られて

も、他の鍵が有効であり、記録媒体全体のコンテンツが盗用される自体を回避できる。

【0068】また、記録媒体21に記録されているデータの一部が平文で記録されているので、例えば、イントロを確認する等、音楽の一部を聞くことができる。なお、平文で記録するデータは、各楽曲の先頭部分に限定されず、各楽曲の複数箇所、ポピュラーな箇所等としてもよい。また、一部の曲については全体を平文で、他の曲については全体を暗号化して記録する等してもよい。

【0069】なお、管理センタ11は、この流通システムの要であり、暗号化技術に精通し、且つ、信頼及び信用の高い企業、半公的機関、公的機関が管理センタ11の機能を実現することが望ましい。

【0070】（第2の実施の形態）第1の実施の形態では、公開鍵暗号化方式（プライベート鍵と公開鍵の対を用いる方式）を使用したが、秘密鍵暗号方式（共通鍵方式）を使用することも可能である。以下、秘密鍵暗号方式を使用する場合の流通システムについて説明する。

【0071】この実施の形態のコンテンツ流通システムの構成及び動作は、基本的に図1に示す第1の実施の形態の流通システムの構成及び動作と同様であり、以下の説明では、特徴部分のみを説明する。

【0072】まず、管理センタ11は、コンテンツメーカー13の要請に応じて暗号ファイルフォーマットを設定すると共にコンテンツ別に暗号鍵を暗号化するためのマスタ鍵Kkを生成する。ただし、マスタ鍵Kkは、コンテンツメーカー13にも通知されず、管理センタ11自身で管理される。

【0073】コンテンツメーカー13は、乱数等を発生し、コンテンツ毎に暗号鍵（コンテンツ鍵）Kcoを生成し、各コンテンツを暗号化する。コンテンツメーカー13は、発生したコンテンツ鍵Kcoを管理センタ11に送付する。管理センタ11は、送付されたコンテンツ鍵Kcoをマスタ鍵Kkで暗号化し、暗号化マスタ鍵Kk（Kco）をコンテンツメーカー13に送付する。

【0074】また、管理センタ11は、証明書DVに相当するデータをコンテンツメーカー13に送付する。コンテンツメーカーは、図2に示す構成と同様に、識別コードDIと、平文データDPと、暗号化データDCと、マスタ鍵Kkにより暗号化されたコンテンツ鍵DK（=Kk（Kco））と、コンテンツメーカーの署名DSと、証明書DVを組み合わせることで1曲分のデータを生成し、さらに、これをN曲分組み合わせ、制御コードを付加して1記録媒体25のデータを作成し、記録媒体21に格納する。

【0075】LSIメーカー15は、管理センタ11から、マスタ鍵Kkと署名用センタ公開鍵KPUceを受領し、これを記憶部37に格納して販売する。

【0076】このようにして、製造された記録媒体21に記録されているコンテンツを再生する場合は、第1の実施の形態と同様に、記憶部37に記憶されている署名

用センタ公開鍵KPUceを用いて証明書DVを検証し、証明書DV内に含まれている署名用コンテンツメーカー公開鍵KPUmを用いてコンテンツメーカー13の署名DSを検証する。

【0077】検証の結果、証明書DVと署名DSが有効であると判断されれば、記憶部37に記憶されているマスタ鍵Kkを用いて暗号化Kコンテンツ鍵DK（=Kk（Kco））を復号してコンテンツ鍵Kcoを得て、以後、このコンテンツ鍵Kcoを用いてコンテンツを復号する。

【0078】このような構成によれば、第1の実施の形態に比較して、より簡易な手順で、デジタルコンテンツを暗号化して流通することができ、コストを抑え、再生時に復号に要する時間を短くすることができる。

【0079】（実施の形態の応用例）上記第1及び第2の実施の形態では、各楽曲のデータの一部を平文で、残りの部分を暗号化して記録媒体21に記録したが、楽曲全体を暗号化して記録してもよい。

【0080】また、上記第1の実施の形態では、各楽曲にコンテンツメーカー13の署名DSと管理センタ11の証明書DVを付加したが、これらのデータを付加しなくてもよい。この場合は、署名DSと証明書DVの検証を行うことなく、コンテンツ鍵Kcoを復号し、復号されたコンテンツ鍵Kcoを用いて楽音データを復号し、再生する。

【0081】上記実施の形態では、コンテンツを復号するために、復号LSI31を製造したが、LSIを製造すること自体は必ずしも必要ではなく、例えば、復号用のソフトウェアを再生装置に組み込む等してもよい。この場合は、ソフトウェアの内部に署名検証用の署名用センタ公開鍵KPUceとマスタプライベート鍵KPRk（又は、マスタ鍵Kk）を含ませしておく。このような方式でも、デジタルコンテンツを暗号化して安全に流通させ、且つ、正当権利者が再生することができる。

【0082】上記構成では、記録媒体21には、コントローラ（LSI）を配置しなかったが、例えば、記録媒体21にコントロール用のLSIを配置し、認証用のデータを記録媒体21に格納しておき、この認証用データを用いてコントローラと復号LSI31との間で認証処理等を行うようにしてもよい。この認証処理で、認証できない場合には、デジタル署名が確認できなかった場合と同様にCPU45をリセットし、再生を禁止する。

【0083】また、この記録媒体21のコピー回数を制限するようにしてもよい。この場合には、記録媒体21上にコピー回数を記録する領域を配置し、コピーが行われる度にコピー回数を更新する。

【0084】この発明は音楽データを暗号化して流通させる場合に限定されず、画像等の任意のデジタルコンテンツの流通に有効である。例えば、印刷対象の画像（例えば、ポートレートのフレームの画像等）を記録媒体に格納して流通させ、プリンタ等この記録媒体を装着



して復号L S Iで再生し、印刷対象の画像と合成して印刷してもよい。

【0085】

【発明の効果】以上説明したように、この発明によれば、任意のデジタルコンテンツの不正コピー等を防止し、デジタルコンテンツの適切な流通を可能とする。

【図面の簡単な説明】

【図1】この発明の一実施の形態にかかるデジタルコンテンツ流通システムの基本構成を示すブロック図である。

【図2】図1に示す流通システムで使用する暗号化鍵を説明するための図である。

【図3】図1に示す流通システムで、市場に流通する記録媒体のフォーマットを示す図である。

【図4】図1に示す流通システムで、市場に流通する復号L S I及び再生装置（オーディオ装置）の構成を示すブロック図である。

【図5】記録媒体にデジタルコンテンツを記録する処理を説明するためのフローチャートである。

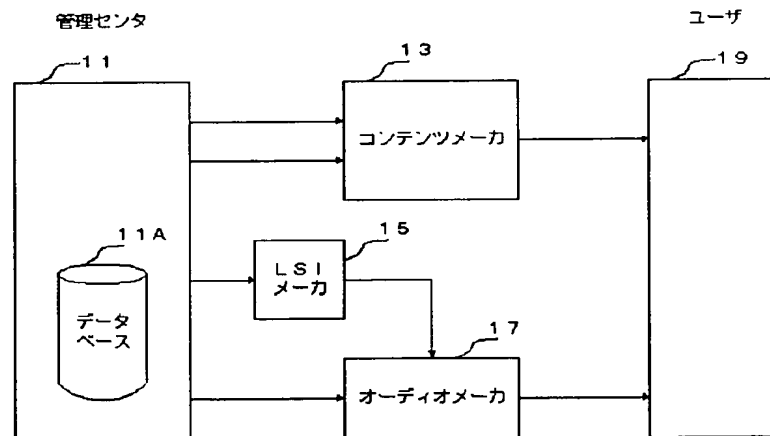
【図6】記録媒体に記録されたデジタルコンテンツを

再生する処理を説明するためのフローチャートである。

【符号の説明】

1 1	管理センタ
1 3	コンテンツメーカ
1 5	L S Iメーカ
1 7	オーディオメーカ
1 9	ユーザ
2 1	記録媒体
3 1	復号L S I
3 3	ドライバ
3 4	署名確認部
3 5	C P Uリセット部
3 6	復号部
3 7	記憶部
3 8	制御部
4 1	コネクタ
4 2	D/A変換器
4 3	スピーカ
4 4	入力部
4 5	C P U

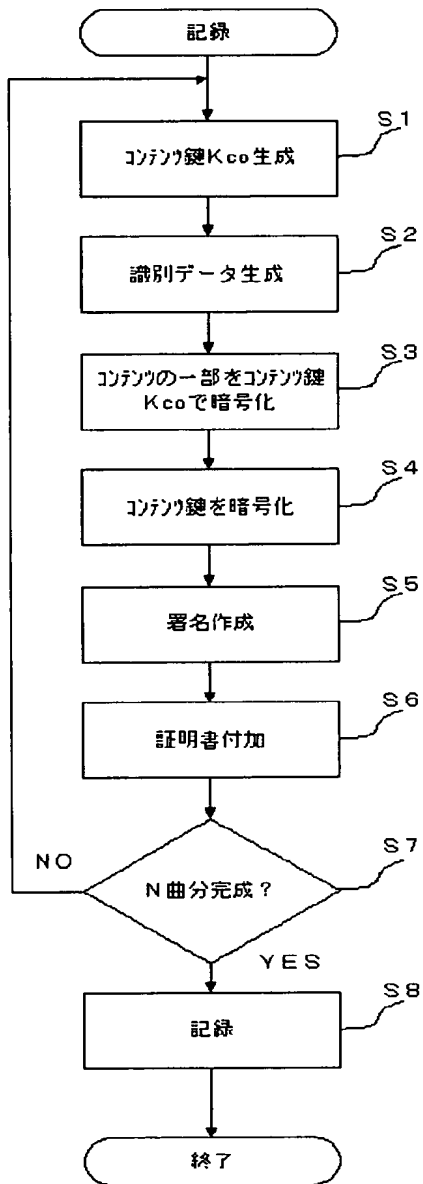
【図1】



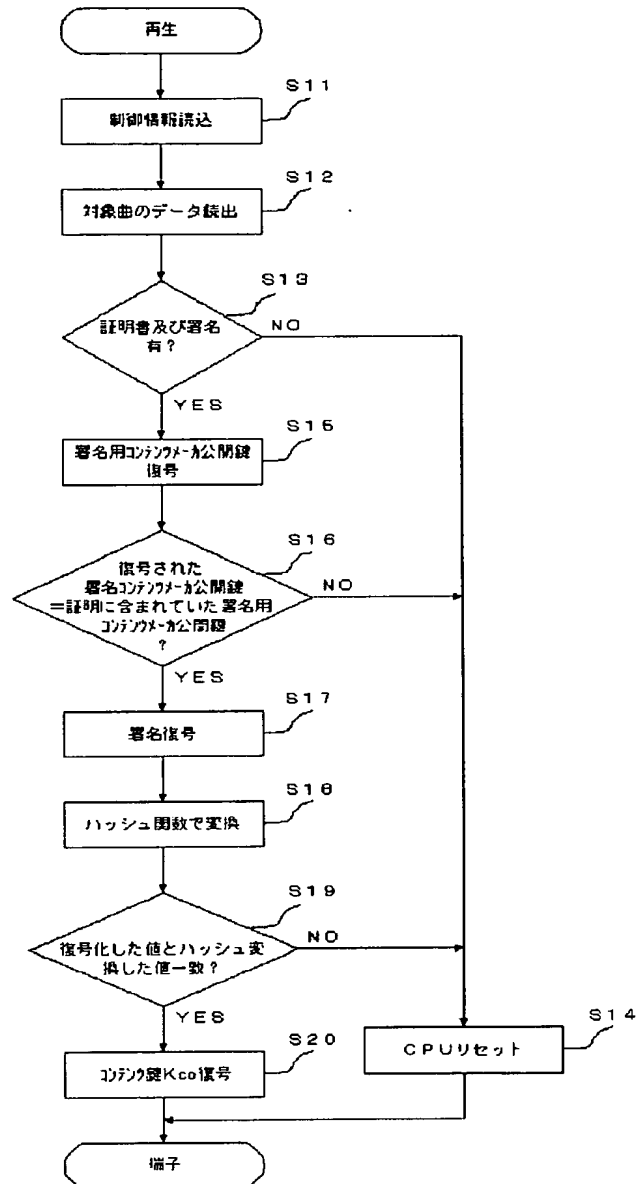
名称	記号	発生者	内容	備考
コンテンツ鍵	K co	コンテンツメーカ	コンテンツを暗号化する	コンテンツ毎に生成される
マスク公開鍵	K PUK	管理センタ	コンテンツ鍵を暗号化する	マスクライバート鍵と対
マスクライバート鍵	K PRk	管理センタ	マスク公開鍵により暗号化されたコンテンツ鍵を復号する	マスク公開鍵と対
署名用コンテンツメーカライバート鍵	K PRm	管理センタ	コンテンツメーカが署名を行う時に使用する	コンテンツメーカ毎に生成される；署名用コンテンツメーカ公開鍵と対
署名用コンテンツメーカ公開鍵	K PUm	管理センタ	コンテンツメーカの署名を検証する際に使用される	コンテンツメーカ毎に生成される；署名用コンテンツメーカライバート鍵と対
署名用センタライバート鍵	K PRce	管理センタ	管理センタがコンテンツメーカの鍵証明書を作成する際に使用する	署名用センタ公開鍵と対
署名用センタ公開鍵	K PUce	管理センタ	コンテンツメーカが鍵証明書内にあるセンタの署名を検証する時に使用する	署名用センタライバート鍵と対

[illegible]

【図5】



【図6】



Japanese Kokai Patent Application No. P2000-22680A

---

Job No.: 228-127514

Ref.: JP2003-37588 & JP2000-22680/PU030241/PPK (Fidez) ORDER NO. 159 and NO. 160

Translated from Japanese by the McElroy Translation Company

800-531-9977

[customerservice@mcelroytranslation.com](mailto:customerservice@mcelroytranslation.com)

(19) JAPANESE PATENT OFFICE (JP)		(12) KOKAI TOKUHYO PATENT GAZETTE (A)		(11) PATENT APPLICATION PUBLICATION NO. P2000-22680A (43) Publication Date: January 21, 2000	
(51) Int. Cl. <sup>7</sup> :		Identification Codes:		FI	Theme codes (reference)
H 04L	9/08			H 04 L 9/00	601 B
G 06F	15/00	330		G 06 F 15/00	330 Z
	17/60			G 09 C 1/00	620 Z
G 09C	1/00	620			640 C
		640		G 06 F 15/21	330
Examination Request: Not filed				No. of Claims: 7 (Total of 11 pages; OL)	
(21) Filing No.: Hei 10[1998]-191706				(71) Applicant: 598090519 KK Open Loop 1-18-5 Kiyota 7-jo, Kiyota-ku, Sapporo-shi, Hokkaido	
(22) Filing Date: July 7, 1998				(72) Inventor: Kazunori Asada KK Open Loop 2-5-5 Kitano 7-jo, Kiyota-ku, Sapporo-shi, Hokkaido	
				(74) Agent: 100095407 Mitsuru Kimura, patent attorney and 2 others	

(54) [Title] DIGITAL CONTENT DISTRIBUTION METHOD AND RECORDING MEDIUM ON WHICH CONTENT IS REPRODUCIBLY RECORDED

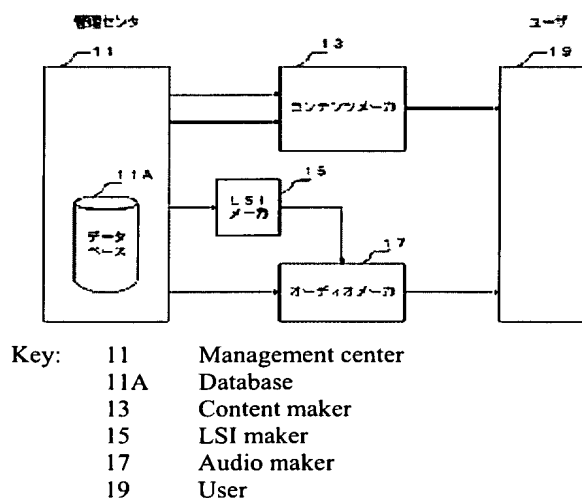
(57) Abstract

Problem

To prevent unauthorized copying and use of music or other digital content and distribute securely.

Means to solve

A management center 11 supplies a master public key KPUk to a content maker, and supplies a master private key KPRk to an LSI maker 15. Content maker 13 records data encrypted by generating a content encryption key Kco according to the content, data in which content encryption key Kco is encrypted using master public key KPUk, and a certificate DV from management center 11 on a recording medium 21. LSI maker 15 includes master private key KPRk for decoding the encrypted content encryption key in a decoding LSI. The decoder decodes the content encryption key using master private key KPRk and decodes the content using the decoding LSI, when the certificate DV and a signature DS on the mounted recording medium 21 are both determined to be valid.



### Claims

1. A method to distribute digital content using a distribution system provided with a management center that manages the distribution of the digital content, a content maker that encrypts and distributes the digital content under the management of the aforementioned management center, and a decoding means providing means that provides a decoding means to decode and make usable the content provided by the aforementioned content maker,

the digital content distribution method being characterized in that:

the aforementioned content maker records content encrypted with a content encryption key, and an encrypted content encryption key on a recording medium and distributes the same,

the aforementioned management center provides decoding information for decoding the encrypted content encryption key to the decoding means providing means,

the aforementioned decoding means providing means includes decoding information for decoding the aforementioned encrypted content encryption key in the aforementioned decoding means,

and the aforementioned decoding means decodes the aforementioned decoding information using the content encryption key recorded on the aforementioned recording medium, and decodes and reproduces the content with the decoded encryption key.

2. The digital content distribution method described in Claim 1, characterized by the fact that:

the aforementioned content maker generates the content encryption key according to the content and encrypts the content, encrypts the generated content encryption key with a master public key supplied from the management center, creates its own signature using a content maker private key for signatures supplied from the management center, and stores the encrypted content, the encrypted content encryption key, the signature and a certificate supplied from the management center on a recording medium,

the aforementioned decoding means providing means includes a master private key for decoding the encrypted content encryption key and a center private key for signatures for authenticating the certificate in the aforementioned decoding means,

the aforementioned decoding means obtains the content maker public key for signatures for the content maker by authenticating the certificate using the center public key for signatures and authenticates the signature with that, and decodes the encrypted content encryption key with the aforementioned master private key and decodes the content with the decoded content encryption key, when the certificate and the signature are both determined to be valid,

the aforementioned management center supplies the master public key, and a certificate that includes information in which the content maker public key for signatures for the content maker is encrypted with the center private key for signatures, to the content maker, and supplies

the master private key and the center private key for signatures to the aforementioned decoding means providing means.

3. The digital content distribution method described in Claim 1, characterized by the fact that:

the aforementioned content maker generates a content encryption key according to the content and encrypts the content, supplies the generated content encryption key to the management center, creates its own signature using a content maker private key for signatures supplied from the management center, and records the content encryption key encrypted with the master encryption key supplied from the management center, the signature, and a certificate supplied from the management center on a recording medium,

the aforementioned decoding means providing means includes a master encryption key, and a center public key for signatures for authenticating the certificate in the aforementioned decoding means,

the aforementioned decoding means obtains the content maker public key for signatures for the content maker by authenticating the certificate using the center management key for signatures and authenticates the signature with that, and decodes the encrypted content encryption key with the aforementioned master encryption key and decodes the content with the decoded content encryption key, when it is determined that the certificate and the signature are both valid,

and the aforementioned management center supplies the certificate that includes information in which the content maker public key for signatures for the content maker is encrypted with the center private key for signatures, and data in which the content encryption key supplied from the content maker is encrypted with the master encryption key to the content maker, and supplies the master encryption key and the center public key for signatures to the aforementioned decoding means providing means.

4. The digital content distribution method described in Claim 1, 2 or 3, characterized by the fact that:

the aforementioned decoding means

is provided with at least an LSI (large scale integrated circuit) that stores information for decoding the aforementioned encrypted content encryption key, decodes the content encryption key using this information, and decodes the encrypted content using the decoded content encryption key,

or with software that includes information for decoding the aforementioned encrypted content encryption key, decodes the content encryption key with the information, and decodes the encrypted content using the decoded content encryption key.

5. The digital content distribution method described in Claim 1, 2, 3 or 4, characterized by the fact that:

the aforementioned content maker

records on the aforementioned recording medium a part of each content [unit] with plain text, and records at least another part encrypted with the aforementioned content encryption key.

6. A digital recording medium, which is a recording medium on which multiple digital content [units] are recorded, and which is characterized by the fact that:

for each digital content [unit],

digital content, at least a part of which is encrypted with a first encryption key according to the content,

the aforementioned first encryption key that is encrypted with a second encryption key,

a digital signature generated using a manufacturer's private key,

and a certificate for a prescribed relationship that includes a public key for the manufacturer in order to authenticate the aforementioned manufacturer's digital signature are recorded.

7. The digital content recording medium described in Claim 6, characterized by the fact that for each digital content [unit], at least a part is recorded on the recording medium with plain text, and at least another part is encrypted with the first encryption key.

#### Detailed explanation of the invention

[0001]

Technical field of the invention

This invention relates to a digital content distribution method and to digital content with which it is possible to achieve a balance between the protection and use of content that is protected by copyrights, etc.

[0002]

Prior art

It is becoming possible for various types of content to be processed, edited and copied due to advances in digital image processing technology. When content processing, editing and copying are haphazardly allowed, however, copyrights and portrait rights may not be protected, and benefits to the rights holder may be diminished. On the other hand, when use of the content is too restricted, the content becomes unusable.



[0003]

To satisfy these requirements, digital watermarks and other technologies have been proposed, but data processing is complicated, and a complicated system is required. For this reason, these are not considered to be systems that can be used easily from the standpoint of a user who is unfamiliar with digital processing technology.

[0004]

Problems to be solved by the invention

This invention was devised in consideration of the aforementioned situation, and has the objective of achieving balance between the use and protection of digital content.

[0005]

Means to solve the problems

In order to accomplish the aforementioned objective, the digital content distribution method pertaining to a first viewpoint of this invention is a method to distribute digital content using a distribution system provided with a management center (11) that manages the distribution of the digital content, a content maker (13) that encrypts the digital content and distributes it under the management of aforementioned management center (11), and decoding means providing means (15, 17) that provide decoding means that can decode and use the content provided by aforementioned content maker (13), and is characterized by the [following] facts. Aforementioned content maker (13) encrypts content with a content encryption key (Kco) generated according to the content. Aforementioned management center (11) provides information (KPUk; Kk) for recording the encrypted content encryption key (KPUk (Kco); Kk (Kco)) on a recording medium (21) to content maker (13). Aforementioned content maker (13) distributes content (DC) encrypted with content encryption key (Kco) and the encrypted content encryption keys (KPUk (Kco); Kk (Kco)) recorded on recording medium (21). Aforementioned management center (11) provides decoding information (KPRk; Kk) for decoding encrypted content encryption keys (KPUk (Kco); Kk (Kco)) to decoding means providing means (15). Aforementioned decoding means providing means (15) includes decoding information (KPRk; Kk) for decoding the aforementioned encrypted content encryption keys in the aforementioned decoding means (LSI etc.). Aforementioned decoding means (LSI etc.) decodes content encryption key (Kco) recorded on aforementioned recording medium (21) using aforementioned decoding information (KPRk; Kk), and decodes and reproduces the content with decoded encryption key (Kco).

[0006]

With this method, the digital content is distributed in an encrypted state to prevent unauthorized use, and in addition, it can be reproduced. The reliability and security of the keys are high, since they are managed by a third party, primarily the management center. In addition, the encryption keys differ according to the content, so even if a specific encryption key is broken, the entire recording medium will not be affected, which is secure.

[0007]

When a public key scheme is used as the encryption scheme, the following configuration is effective. First, the aforementioned content maker generates a content encryption key according to the content and encrypts the content, encrypts the generated content encryption key with a master public key (KPUk) supplied from the management center, generates its own signature using a content maker private key (KPRm) for signatures supplied from management center (11), and stores the encrypted content, encrypted content encryption key (KPUk (Kco)), signature (DS) and a certificate (DV) supplied from management center (11) on recording medium (21). Aforementioned decoding means supplying means (15) includes a master private key (KPRk) for decoding encrypted content encryption key (KPUk (Kco)) and a center public key (KPUce) for signatures for authenticating certificate (DV) in aforementioned decoding means (LSI). Aforementioned decoding means (LSI) obtains a content maker public key (KPUm) for signatures for content maker (13) by authenticating certificate (DV) using center public key (KPUce) for signatures and authenticates signature (DS) with it, and decodes encrypted content encryption key (KPUk (Kco)) with aforementioned master private key (KPRk) and decodes the content with decoded content encryption key (Kco), when it is determined that certificate (DV) and signature (DS) are both valid. Aforementioned management center (11) supplies master public key (KPUk) and certificate (DV) that includes information (KPRce (KPUm) in which content maker public key (KPUm) for signatures for the content maker is encrypted with center private key (KPRce) for signatures to the content maker, and supplies master private key (KPRk) and center public key (KPUce) for signatures to aforementioned decoding means providing means (15). With this method, the key for encrypting the content encryption keys and the key for decoding are managed separately, so the method is more secure. In addition, the reliability is high due to the fact that a signature and a certificate are used.

[0008]

When a secret key scheme is used as the encryption scheme, the following configuration is effective. Aforementioned content maker (13) generates a content encryption key (Kco) according to the content and encrypts the content, supplies generated content encryption key

(Kco) to management center (11), creates its own signature (DV) [sic; (DS)] using a content maker private key (KPRm) for signatures supplied from management center (11), and records the encrypted content (DC), a content encryption key (Kk (Kco)) encrypted with a master encryption key (Kk) supplied from management center (11), signature (DV) [sic; (DS)] and a certificate (DV) supplied from the management center on recording medium (21). Aforementioned decoding means providing mean (15) includes master encryption key (Kk) and a center public key (KPRce) for signatures for authenticating certificate (DV) in aforementioned decoding means (LSI). Aforementioned decoding means (LSI) obtains a content maker public key (KPUm) for signatures for the content maker by authenticating certificate (DV) using center public key (KPRce) for signatures and authenticates signature (DS) with that, and decodes encrypted content encryption key (Kk (Kco)) with aforementioned master encryption key (Kk) and decodes the content with decoded content encryption key (Kco), when it is determined that certificate (DV) and signature (DS) are both valid. Aforementioned management center (11) supplies certificate (DV) that includes information (KPRce (KPUm)) in which content master public key (KPUm) for signatures for content maker (13) is encrypted with center private key (KPRce) for signatures, and data in which content encryption key (Kco) supplied from content maker (13) is encrypted with master encryption key (Kk) to content maker (13), and supplies master encryption key (Kk) and center public key (KPUce) for signatures to aforementioned decoding means providing means (15).

[0009]

With this method, the key for encrypting the content encryption keys and the key for decoding are the same, and processing when decoding (reproducing) can be accomplished quickly, which is particularly useful for applications where real time characteristics are required. In addition, processing to encrypt the content encryption keys is performed by the center, so the reliability is very high while a secret key scheme is used. Additionally, the reliability is high due to the fact that a signature and a certificate are used.

[0010]

The aforementioned decoding means could be an LSI that stores information (KPRk, Kk) for decoding aforementioned encrypted content encryption key (Kco), decodes content encryption key (Kco) with this information, and decodes the encrypted content using decoded content encryption key (Kco), or it could be software that includes information for decoding the aforementioned encrypted content encryption key, decoding content encryption key (Kco) with this information, and decoding the encrypted content using decoded content encryption key (Kco).

[0011]

The aforementioned content maker could also record a part of each content [unit] with plain text, and record at least another part encrypted with aforementioned content encryption key (Kco) on the aforementioned recording medium. If so, opening a part of a song, the intro for example, to identify the song, the allowance of commercial use, and other actions can easily be accomplished.

[0012]

In order to accomplish the aforementioned objective, a recording medium on which multiple digital content [units] are recorded and that pertains to a second viewpoint of this invention is characterized by the fact that, for each content [unit], digital content, at least a part of which is encrypted with a first encryption key (Kco) according to the content, aforementioned first encryption key (Kco) that is encrypted with a second encryption key (KPUk; Kk), a digital signature (DS) generated using the manufacturer's private key, and a certificate (DV) for a prescribed relationship that includes the manufacturer's public key (KPUm) for authenticating the aforementioned manufacturer's digital signature are recorded.

[0013]

With this configuration, anyone other than someone who has information to verify the certificate and information to decode the first key, that is, anyone who does not have an authorized right, is unable to verify the authenticity of the prescribed relationship, as well as verify the manufacturer's signature from the verification result and then decode the content. Therefore, it is possible for digital data to be distributed securely on the market.

[0014]

For each digital content [unit], a part could be recorded in plain text, and at least another part could be encrypted with the first encryption key.

[0015]

Embodiments of the invention

The content distribution system and method pertaining to an embodiment of this invention will be explained using a case in which audio data (music data) are distributed as an example.

#### First embodiment

The content distribution system in this embodiment, as shown in Figure 1, includes a management center 11, a content maker 13, an LSI (large scale integrated circuit) maker 15, an audio maker (audio device maker) 17, and a user 19.

[0016]

Management center 11 has encryption technology and sets the encrypted file format according to the properties of the content to be encrypted and customer requirements, while also generating various types of encryption keys, which are supplied to content maker 13 and LSI maker 15. Management center 11 records and manages encrypted file formats and encryption keys according to the customer or contract using a database 11A. The encryption keys generated by management center 11 will be collectively explained referring to Figure 2.

[0017]

Content maker 13 generates an encryption key for each content [unit] and encrypts the content (here, music data) based on usage permission for the encrypted file formats from management center 11, and saves them on a recording medium (a flash memory, for example), which is sold.

[0018]

LSI maker 15 designs, manufactures and sells a decoding LSI to decode the encrypted content in accordance with the encryption file format set by management center 11 and the provided encryption key, using an ASIC (integrated circuit for specific applications), based on usage permission for the encrypted file format from management center 11.

[0019]

The decoding LSI is sold to audio maker 17. Audio maker 17 incorporates the decoding LSI, based on the usage permission for the encrypted file format from management center 11, decodes the content data recorded on the medium provided by content maker 13, and manufactures and sells the reproducing device (audio device).

[0020]

Management center 11 is operated using compensation from content maker 13, LSI maker 15 and audio maker 17 as all or a part of the operating funds.

[0021]

User 19 purchases an audio device provided by audio maker 17 and a recording medium on which are stored music data provided by content maker 13, and mounts the recording medium in the audio device to reproduce the music data. The music data reproduced from the recording medium are encrypted data, and they are decoded by the decoding LSI and reproduced as music.

[0022]

Next, each of the encryption keys used with this distribution system will be explained referring to Figure 2. Content key Kco is an encryption key generated by content maker 13 generating a random number for each content [unit], and the content maker uses it for encrypting the content to be distributed.

[0023]

Master public key KPUk is an encryption key generated and supplied by management center 11 for each content maker (can also be for each content [unit], etc.), and is used by content maker 13 to which it is supplied to encrypt content key Kco.

[0024]

Master private key KPRk is an encryption key generated by management center 11 and paired with master public key KPUk, and is supplied to each LSI maker 15. It is stored in the decoding LSI or in decoding software, and is used for decoding content key Kco that has been encrypted with master public key KPUk.

[0025]

Content maker private key KPRm for signatures is an encryption key generated and provided by management center 11 for each content maker. It is used for the content maker to sign each content [unit].

[0026]

Content maker public key KPUM for signatures is generated by management center 11 and paired with content maker private key KPRm for signatures. It is used while included in a certificate issued by management center 11 in order to authenticate the content maker signature.

[0027]

Center private key KPRce for signatures is generated independently by management center 11, and is used to encrypt content maker public key KPUm for signatures for each content maker and generate a "content maker key certificate."

[0028]

Center public key KPUce for signatures is a key generated by management center 11 and paired with center private key KPRce for signatures. It is stored in the decoding LSI and is used to authenticate the signature of management center 11 within the "content maker key certificate."

[0029]

Next, the music data provided by content maker 13 will be explained. An example of the music data stored on recording medium 21 is shown in Figure 3. At the beginning position on each medium, the medium's identification code, an identification code for content maker 13, the medium type, TOC (TABLE OF CONTENTS) information, control information DZ, such as copyright information, and data for N songs' worth of music are recorded.

[0030]

The data for each song are configured from an identification code DI, plain text data DP, encrypted data DC, encrypted content key DK, content maker signature DS, and certificate DV.

[0031]

Identification code DI consists of non-encrypted plain text data that indicate the name, song code, performance time, etc. of each song.

[0032]

Plain text data DP consist of non-encrypted plain text data for a prescribed time (around 10 sec, for example) in the first half of the song data.

[0033]

Encrypted data DC are data generated by encrypting the last half portion of the song data with content key Kco for the content.

[0034]

Encrypted content key DK consists of data KPUk (Kco) obtained by encrypting content key Kco with master public key KPUk.

[0035]

Content maker signature DS consists of data KPRm (H (DI; DP; DC; DK)) obtained by converting identification code DI, plain text data DP, encrypted data DC, and encrypted content key DK with a hash function or another one-way function H() and encrypting this with content maker private key KPRm.

[0036]

Key certificate DV includes content maker public key KPUM for signatures, and data KPRce (KPUM) obtained by encrypting content maker public key KPUM for signatures with center private key KPRce for signatures, and is for the purpose of management center 11 certifying that the key used by the content maker for the signature is valid.

[0037]

Next, the decoding LSI will be explained. Decoding LSI 31, as shown in Figure 4, is provided with a driver 33, a signature verification unit 34, a CPU reset unit 35, a decoding unit 36, a storage unit 37, and a control unit 38.

[0038]

Driver 33 successively reads the recorded data on recording medium 21. Signature verification unit 34 determines whether certificate DV and signature DS have been attached to the content to be decoded, and authenticates certificate DV and signature DS when it is determined that they attached.

[0039]

Specifically, signature verification unit 34 decodes portion KPRce (KPUM) that is encrypted within certificate DV read by driver 33 using center public key KPUCe for signatures from management center 11 stored in storage unit 37, and obtains content maker public key KPUM for signatures. Signature verification unit 34 compares decoded content maker public key KPUM for signatures and the plain-text content maker public key KPUM for signatures and determines whether they match.

[0040]

When it is determined that they match, content maker signature DS is authenticated using content maker public key KPUM for signatures. Specifically, whether signature DS decoded using content maker public key KPUM for signatures, identification code DI, plain text data DP,



encrypted data DC and encrypted content key DK converted with a prescribed one-way function  $H()$  match is determined. When signature verification unit 34 determines that they match, encrypted content key DK (=KPUk (Kco)) is decoded using master private key KPRk, and content key Kco is reproduced.

[0041]

CPU reset unit 35 resets CPU 45 of the device in which decoding LSI 31 is incorporated (reproducing device) to prohibit data reproduction when signature verification unit 34 cannot detect a signature or certificate (no signature or certificate is present) and when authentication cannot be certified (present, but cannot be certified). The reproduction operation is canceled by this.

[0042]

Decoding unit 36 is the portion that decodes the data read by driver 33 when signature verification unit 34 certifies the signature, and reproduces the plain text data without changes and decodes music data DD for the encrypted data using content key Kco decoded by signature verification unit 34. Storage unit 37 stores center public key KPUce for signatures for management center 11 and a master private key KPRk for each content maker 13.

[0043]

In order for the system to be operated effectively, it is necessary for keys KPUce and KPRk stored by storage unit 37 to be kept strictly secret. For this reason, storage unit 37 is connected to the signature verification unit using an internal bus that is different from the other common buses so as not to be directly accessible from outside decoding LSI 31. Data for the keys are also not output unchanged to the outside.

[0044]

Control unit 38 controls the operation of each unit in decoding LSI 31.

[0045]

Next, the configuration of the audio device that uses decoding LSI 31 will be explained. As shown in Figure 4, the audio device is configured with a connector 41 where the recording medium can be detachably mounted, aforementioned decoding LSI 31 that is connected to recording medium 21 through connector 41, a D/A converter 42 that converts the music data output from decoding LSI 31 to analog data, a speaker (including headphones, etc.) 43 that

produces sound from the analog signals output by D/A converter 42, an input unit 44, and a CPU (control unit) 45 that controls all operations of the audio device.

[0046]

Recording medium 21 is detachably mounted in connector 41. D/A converter 42 converts the reproduced digital audio signal to an analog audio signal and outputs it. Speaker 43 produces sound from the analog audio signal. CPU 45 controls all operations of the system, including the reading and reproduction of data from recording medium 21, in accordance with input from input unit 44.

[0047]

Next, a digital content distribution method that uses the distribution system will be explained. Content maker 13 that wants to manufacture recording media 21 on which music is recorded, and audio maker 17 that wants to manufacture audio devices to play the recording media are registered at management center 11.

[0048]

When use of the encrypted file format is permitted for a content maker 13, management center 11 permits use of the encrypted file format, provides the knowhow for this, and also provides the paired master public key  $KPU_k$  and private key  $KPR_m$  for signatures. A certificate ( $KPU_m: KPR_{ce}(KPU_m)$ ) comprising content maker public key  $KPU_m$  for certification and data  $KPR_{ce}(KPU_m)$  in which content maker public key  $KPU_m$  for certification is encrypted using center private key  $KPR_{ce}$  for signatures is created and is sent to content maker 13. Content maker 13 pays a fixed royalty (compensation) to management center 11.

[0049]

When manufacture of a decoding LSI conforming to the encrypted file format is permitted for an LSI maker 15, management center 11 provides the permission and the knowhow, and also notifies the master private key  $KPR_k$  for each content maker and center public key  $KPU_{ce}$  for its own signature. LSI maker 15 pays a fixed royalty to management center 11.

[0050]

In addition, when use of the encrypted file format is permitted for an audio maker 17, management center 11 gives permission to use the encrypted file format and also provides the knowhow for it. Audio maker 17 pays a fixed royalty to management center 11.

[0051]

The operation of recording content to recording medium 21 by a content maker will be explained below referring to the flow chart in Figure 5. First, content maker 13 generates a random number for each content [unit], that is, each song, stored on the recording medium, for example, and generates a content key  $K_{co}$  (step S1). Next, song identification code and control code identification data  $DI$  are generated (step S2).

[0052]

Additionally, a prescribed amount of the beginning portion  $DP$  of the songs to be recorded is left as plain text, and the remaining portion  $DC$  is encrypted with content key  $K_{co}$  (step S3). Content key  $K_{co}$  generated at step S1 is encrypted with master public key  $KPU_k$  and encrypted content key  $DK$  is generated (step S4).

[0053]

Additionally, all of the abovementioned data, that is, identification data  $DI$ , plain text data  $DP$ , encrypted data  $DC$ , and encrypted (that has been encrypted) content key  $KPU_k$  ( $K_{co}$ ) are converted using a hash function or another one-way function  $H()$ . The conversion result is additionally encrypted with content maker private key  $KPR_m$  for signatures, and a content maker signature ( $=KPR_m(H(DI; DP; DC; KPU_k(K_{co}))$ ) is generated (step S5).

[0054]

Certificate  $DV$  provided from management center 11 is additionally added to the data above (step S6), and the data for 1 song are complete. Content maker 13 combines data for 1 song that are generated in this way are combined in  $N$  songs' worth as appropriate (step S7), data for 1 recording medium are generated, they are recorded on recording medium 21 (step S8), and [the medium] is distributed on the market (sold). Note that once the data to be recorded are created in memory, processing is finished just by the data being recorded on the recording medium.

[0055]

At the same time, LSI maker 13 [sic; 15] that has received permission manufactures a decoding LSI 31 provided with driver 33, etc. in accordance with the provided format using ASIC technology, etc. In this instance, center public key  $KPU_{ce}$  for signatures for management center 11, and the pair of identification code and master private key  $KPR_k$  for content maker 13 are recorded in storage unit 37.

[0056]

Audio maker 15 [sic; 17] that has received permission purchases decoding LSI 31 from LSI maker 15 and manufactures an audio device as shown in Figure 4.

[0057]

A user 19 who purchases an audio device from audio maker 17 and a recording medium from content maker 13 mounts recording medium 21 in connector 41 of the audio device as shown in Figure 4.

[0058]

Next, content reproduction is performed with the steps shown in the flow chart in Figure 6. First, when reproduction is instructed and a song number is designated from input unit 44, CPU 45 controls driver 33 of decoding LSI 31 and data are read, the song's position and the content maker identification code are identified from control information DZ (step S11), and all the data for the song are read from the relevant storage position (step S12).

[0059]

Signature confirmation unit 34 determines whether certificate DV for management center 11 and signature DS for content maker 13 have been attached to the content to be decoded (reproduced) (step S13). When it is determined that at least one has not been attached, CPU 45 is reset through CPU reset unit 35 in order to prevent content reproduction (step S14). On the other hand, when it is determined at step S13 that certificate DV and signature DS have been attached, certificate DV and signature DS are authenticated (steps S15-S21).

[0060]

Specifically, signature verification unit 34 decodes the portion KPRce (KPUm), where content maker public key KPUm for signatures that is encrypted with center private key KPRce for signatures, within certificate DV read by driver 33, with center public key KPUce for signatures that is saved in storage unit 37 (step S15), and determines whether it matches the content maker public key KPUm for signatures saved with plain text in certificate DV (step S16). When it is determined that they do not match, certificate DV is invalid, and CPU 45 is reset (step S14).

[0061]

On the other hand, when it is determined at step S16 that they do match, certificate DV is valid, and signature DS is authenticated using content maker public key KPUM for signatures included in certificate DV.

[0062]

First, the signature is decoded using content maker public key KPUM for signatures (step S17). Next, identification code DI, plain text data DP, encrypted data DC, and encrypted content key DK are converted with prescribed hash function H() (step S18).

[0063]

Next, whether the content decoded at step S17 and the data converted with hash function H() at step S18 match is determined (step S19). If they do not match, the signature is invalid, and CPU 45 is reset (step S14).

[0064]

When it is determined at step S19 that they do match, that is, that both certificate DV and signature D are valid (the encryption key is correct), signature verification unit 34 decodes encrypted content key DK (= KPUK (Kco)) using master private key KPRk for content maker 13 that was saved in storage unit 37, and content key Kco is reproduced (step S20).

[0065]

Signature verification unit 34 provides decoded content key Kco to decoding unit 36 and also outputs a decode instruction signal.

[0066]

Decoding unit 36 responds to the decode instruction signal, outputs the plain text data for each song read by driver 33 without change, and decodes encrypted portion DC using content key Kco and outputs it. The output data are converted to an analog signal by D/A converter 47, and sound is produced from speaker 48.

[0067]

With such a configuration, digital content is encrypted and distributed, and can be reproduced only with a device that has a specialized LSI, so unauthorized copying of the digital content can be prevented. In addition, it is possible for essentially anyone to manufacture/sell products that conform to the common encrypted file format just by registering at management

center 11. Additionally, the encryption keys differ by content units, so even if some of the encryption keys are broken, the other keys are valid, and a thing itself [sic; situation] where the content of the entire recording medium will be pirated can be avoided.

[0068]

In addition, a part of the data recorded on recording medium 21 is recorded with plain text, so a part of the music can be heard, for example, the intro can be verified. Note that the data recorded with plain text are not limited to the beginning portion of the individual songs, but could also be multiple locations within each song, popular locations, etc. In addition, some of the songs could be completely recorded with plain text, and the other songs could be completely encrypted.

[0069]

Note that management center 11 is required for this distribution system, and it is preferable that businesses, semi-public institutions and public institutions that are conversant in encryption technology, and that are highly reliable and trustworthy, realize the functions of management center 11.

[0070]

Second embodiment

With the first embodiment, a public key encryption scheme (scheme using a pair of a private key and a public key) was used, but a secret key encryption scheme (common key scheme) can also be used. A distribution system in which a secret key encryption scheme is used will be explained below.

[0071]

The configuration and operation of the content distribution system in this embodiment are basically the same as the configuration and operation of the distribution system in the first embodiment shown in Figure 1, and in the explanation below, only the distinctive portions will be explained.

[0072]

First, management center 11 sets the encrypted file format according to a request by content maker 13 and also generates master key Kk for encrypting the encryption key according to the content. Here, content maker 13 is not notified of master key Kk and is managed by management center 11.

[0073]

Content maker 13 generates random numbers, generates encryption key (content key) Kco for each content [unit], and encrypts each content [unit]. Content maker 13 sends the generated content key Kco to management center 11. Management center 11 encrypts the content key Kco that was sent with master key Kk and sends encrypted master key Kk (Kco) to content maker 13.

[0074]

Management center 11 also sends data corresponding to certificate DV to content maker 13. The content maker generates data for 1 song by combining identification code DI, plain text data DP, encrypted data DC, content key DK encrypted with master key Kk (=Kk (Kco)), content maker signature DS, and certificate DV, identical to the configuration shown in Figure 2, and additionally combines N songs' worth of this, adds controls codes to generate data for 1 recording medium 25, and saves on recording medium 21.

[0075]

LSI maker 15 receives master key Kk and center public key KPUce for signatures from management center 11 and saves them in storage unit 37, which is sold.

[0076]

When content recorded on recording medium 21 that is manufactured in this way is reproduced, certificate DV is authenticated using center public key KPUce for signatures stored in storage unit 37, and signature DS of content maker 13 is authenticated using content maker public key KPUM included in certificate DV, in the same way as in the first embodiment.

[0077]

If as a result of authentication, it is determined that certificate DV and signature DS are valid, encrypted K [sic] content key DK (= Kk (Kco)) is decoded using master key Kk stored in storage unit 37 to obtain content key Kco, and the content is decoded thereafter using content key Kco.

[0078]

With such a configuration, digital content can be encrypted and distributed with a simpler procedure, costs can be held down, and the time required for decoding when reproducing can be shortened, in comparison with the first embodiment.

[0079]

Application examples of the embodiments

With the first and second embodiments above, a part of the data for each song is recorded on recording medium 21 with plain text, and the remaining portion is encrypted, but all of the songs could also be encrypted and recorded.

[0080]

In addition, with the first embodiment above, signature DS of content maker 13 and certificate DV for management center 11 are added to each song, but these data need not be added. In this case, content key Kco is decoded and the music data are decoded and reproduced using decoded content key Kco without authenticating signature DS and certificate DV.

[0081]

With the embodiments above, decoding LSI 31 was manufactured to decode the content, but the manufacture of said LSI is not necessarily required. For example, software for decoding could be incorporated into the reproducing device. In this case, center public key KPUce for signatures for signature authentication and master private key KPRk (or master key Kk) are included in the software. With such a scheme as well, digital content can be encrypted and securely distributed, and valid rights holders can reproduce it.

[0082]

With the configuration above, a controller (LSI) was installed for recording medium 21, but, for example, an LSI for control could be installed on recording medium 21, data for verification could be saved on recording medium 21, and verification processing could be carried out between the controller and decoding LSI 31. When verification is not possible with this verification processing, CPU 45 is reset and reproduction is prohibited, as in the case when a digital signature cannot be verified.

[0083]

The number of times recording medium 21 is copied could also be restricted. In this case, a region to record the number of copies is placed on recording medium 21, and the number of copies is updated each time copying is performed.



[0084]

This invention is not limited to cases where music data are encrypted and distributed and is effective for distribution of any digital content, such as images. For example, images to be printed (portrait frame images, for example) could be saved on a recording medium and distributed, and the recording medium could be mounted in a printer or the like and reproduced with a decoding LSI, and printing could be accomplished in combination with the images to be printed.

[0085]

Effect of the invention

As explained above, with this invention, unauthorized copying, etc. of any digital content can be prevented, and appropriate distribution of digital content is enabled.

#### Brief description of the figures

Figure 1 is a block diagram showing the basic configuration of a digital content distribution system pertaining to one embodiment of this invention.

Figure 2 is a figure for explaining the encryption keys used with the distribution system shown in Figure 1.

Figure 3 is a figure for explaining the format of a commercially distributed recording medium distributed, with the distribution system shown in Figure 1.

Figure 4 is a block diagram showing the configuration of the decoding LSI and a commercially distributed reproducing device (audio device), with the distribution system shown in Figure 1.

Figure 5 is a flow chart for explaining processing to record the digital content on the recording medium.

Figure 6 is a flow chart for explaining processing to reproduce the digital content recorded on the recording medium.

#### Explanation of symbols

- 11 Management center
- 13 Content maker
- 15 LSI maker
- 17 Audio maker
- 19 User
- 21 Recording medium
- 31 Decoding LSI

- 33 Driver
- 34 Signature verification unit
- 35 CPU reset unit
- 36 Decoding unit
- 37 Storage unit
- 38 Control unit
- 41 Connector
- 42 D/A converter
- 43 Speaker
- 44 Input unit
- 45 CPU

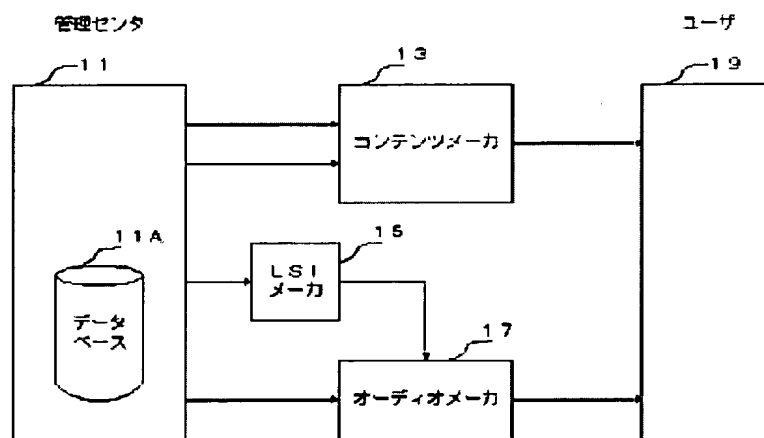


Figure 1

- Key:
- 11 Management center
  - 11A Database
  - 13 Content maker
  - 15 LSI maker
  - 17 Audio maker
  - 19 User

Name	Code	Originator	Content	Remarks
Content key	K co	Content maker	Encrypts content	Generated for each content [unit]
Master public key	K PUK	Management center	Encrypts content key	Paired with master private key
Master private key	K PRk	Management center	Decodes content key encrypted with master public key	Paired with master public key
Content maker private key for signatures	K PRm	Management center	Used when content maker performs [sic; creates] signatures	Generated for each content maker; paired with content maker public key for signatures
Content maker public key for signatures	K PUm	Management center	Used when content maker signature is authenticated	Generated for each content maker; paired with content maker private key for signatures
Center private key for signatures	K PRce	Management center	Used when management center creates key certificate for content maker	Paired with center public key for signatures
Center public key for signatures	K PUce	Management center	Used when content maker authenticates center signature in key certificate	Paired with center private key for signatures

Figure 2

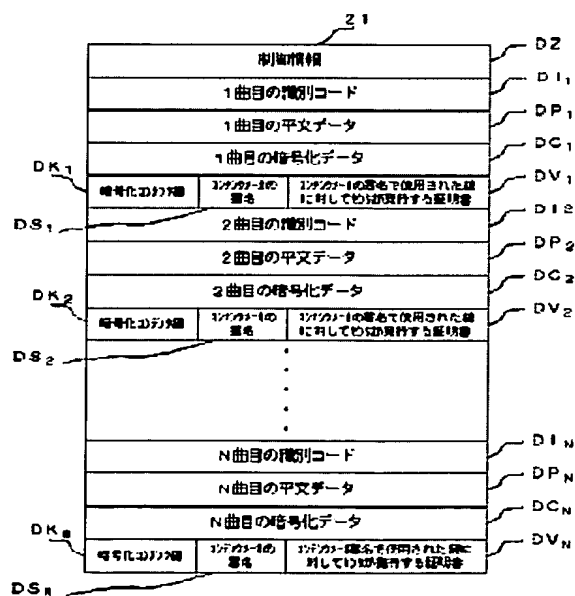


Figure 3

Key:	DZ	Control information
	DI <sub>1</sub>	First song identification code
	DP <sub>1</sub>	First song plain text data
	DC <sub>1</sub>	First song encrypted data
	DK <sub>1</sub>	Encrypted content key
	DS <sub>1</sub>	Content maker's signature
	DV <sub>1</sub>	Certificate issued by center for key used with content maker's signature
	DI <sub>2</sub>	Second song identification code
	DP <sub>2</sub>	Second song plain text data
	DC <sub>2</sub>	Second song encrypted data
	DK <sub>2</sub>	Encrypted content key
	DS <sub>2</sub>	Content maker's signature
	DV <sub>2</sub>	Certificate issued by center for key used with content maker's signature
	DI <sub>N</sub>	Nth song identification code
	DP <sub>N</sub>	Nth song plain text data
	DC <sub>N</sub>	Nth song encrypted data
	DK <sub>N</sub>	Encrypted content key
	DS <sub>N</sub>	Content maker's signature
	DV <sub>N</sub>	Certificate issued by center for key used with content maker's signature

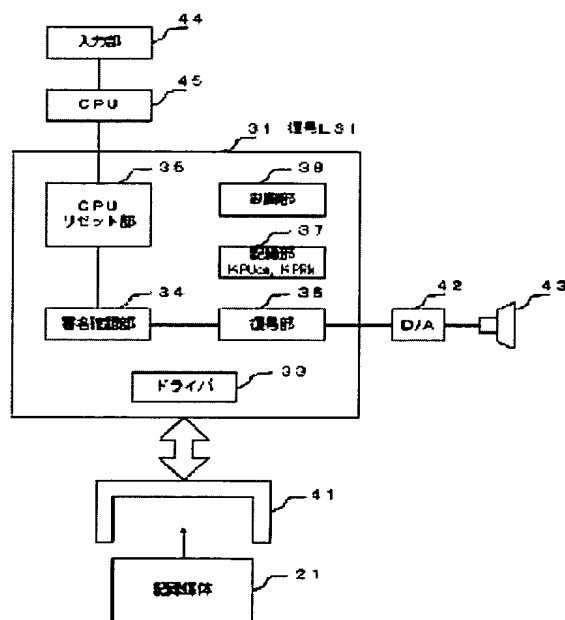


Figure 4

Key:	21	Recording medium
	31	Decoding LSI

33	Driver
34	Signature verification unit
35	CPU reset unit
36	Decoding unit
37	Storage unit
38	Control unit
44	Input unit

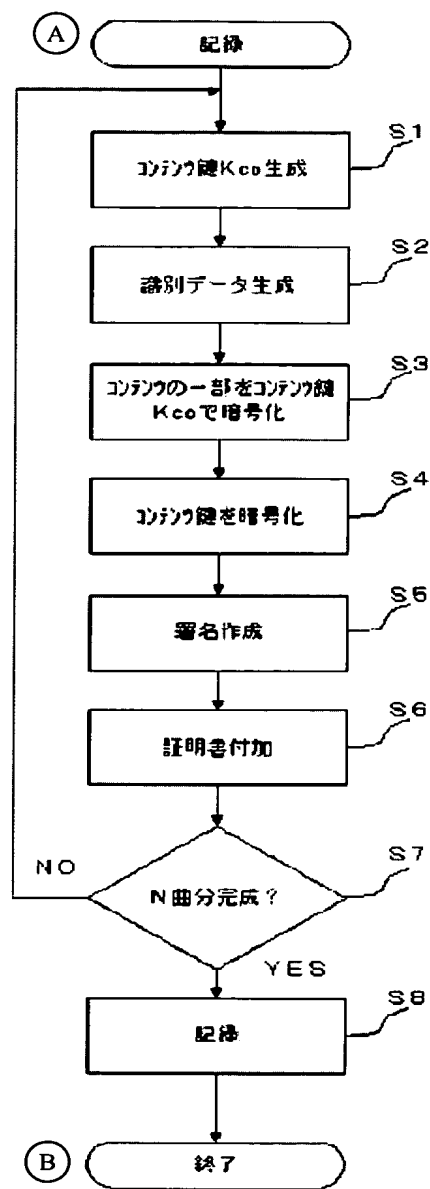


Figure 5

Key: A      Recording  
 B      End  
 S1      Content key Kco generation  
 S2      Identification data generation  
 S3      Part of content is encrypted with content key Kco  
 S4      Content key is encrypted

- S5 Signature creation  
 S6 Certificate addition  
 S7 N songs' worth complete?  
 S8 Recording

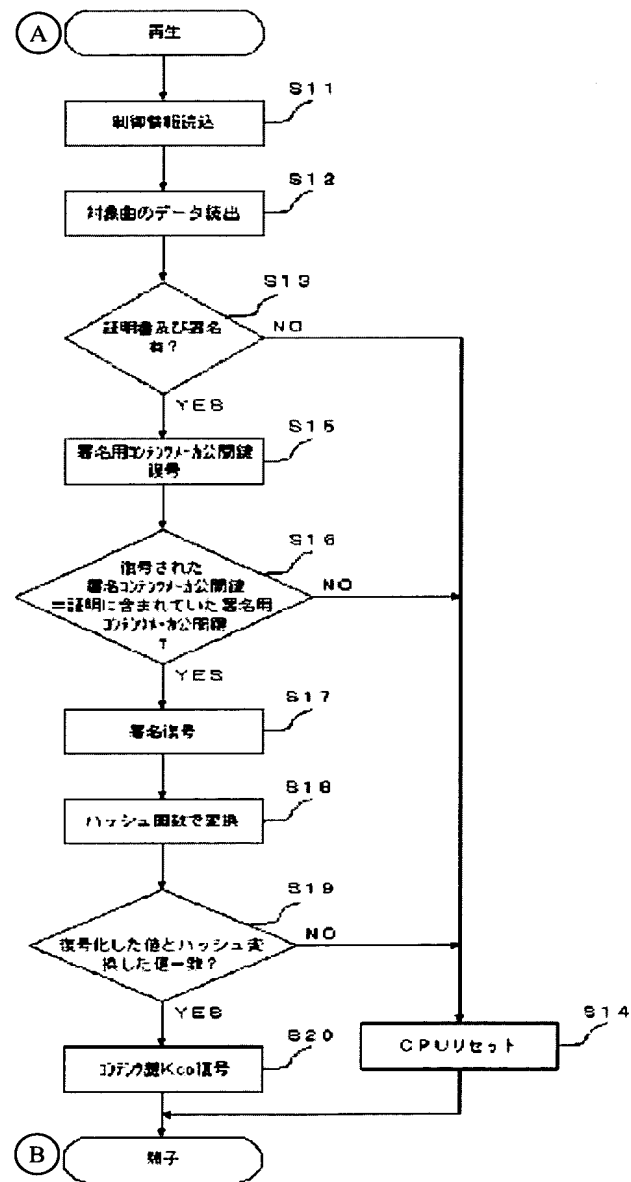


Figure 6

Key: A    Reproduction  
 B    Terminal [sic; End]

- S11 Reading in of control information
- S12 Reading of target song data
- S13 Certificate and signature present?
- S14 CPU reset
- S15 Encryption of content maker public key for signatures
- S16 Decoded content maker public key [for] signatures = content maker public key for signatures included in certificate?
- S17 Signature decoding
- S18 Conversion with hash function
- S19 Do decoded value and hash converted value match?
- S20 Decoding of content key Kco